# **Red Team: Summary of Operations**

## **Table of Contents**

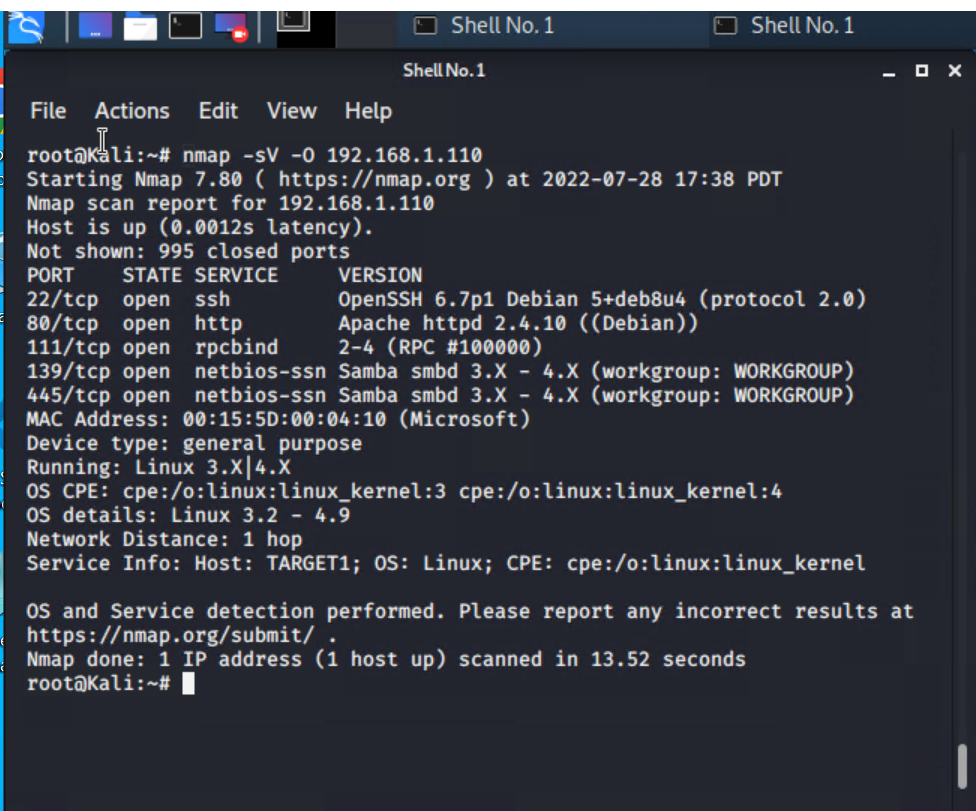
* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

*TODO: Fill out the information below.*

Nmap scan results for each machine reveal the below services and OS details:

$ nmap ... # TODO: nmap -sV -O 192.168.1.110

# TODO: 

This scan identifies the services below as potential points of entry:

* Target 1
  + ssh (port 22)
  + http (port 80)
  + rpcbind (port 111)
  + Netbios-ssn Samba smbd 3.X - 4.X (ports 139 and 445)

*TODO: Fill out the list below. Include severity, and CVE numbers, if possible.*

The following vulnerabilities were identified on each target:

* Target 1

**Port Scanning**

* Using *nmap -sS* to scan a network and obtain ip’s of all machines on network
* Once all ip’s were obtained we used *nmap -sV* to port scan version detect

**Wordpress User Enumeration**

* Using *wpscan* we utilized it to gain username information. The username info was used by the attackers to help gain access to the web server

**Weak Passwords / Open Port 22**

* Using *nmap -sV* we scanned Target 1 and found that port 22, 80, 111, 139 and 445 which would give us access to the machine.
* With the list of users from four *wpscan* we guessed Micheal’s Password and we explored the files and found *Flags 1 & 2*.
* Alternatively you could also use *find . -iname {thisfile.txt}* to search for the flag files if they are in an area that Michael can access.
* Using *john* we also cracked stephen’s password

**MySQL Database Access**

* We were able to discover a file containing login information for the MySQL database. Able to use the login information to gain access to the MySQL database

**Misconfiguration of User Privileges/Privilege Escalation**

* We noticed that Steven had sudo privileges for python. Able to utilize Steven’s python privileges in order to escalate to root

**Apache https 2.4.10**

* Uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials

**open rpcbind port** (<https://nvd.nist.gov/vuln/detail/CVE-2017-8779#vulnCurrentDescriptionTitle> )

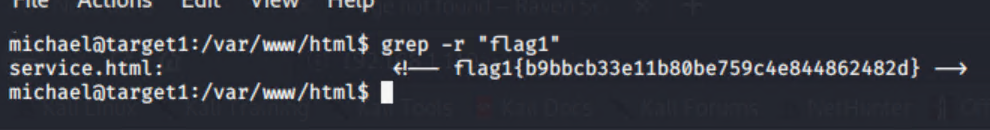
* rpcbind through 0.2.4, LIBTIRPC through 1.0.1 and 1.0.2-rc through 1.0.2-rc3, and NTIRPC through 1.4.3 do not consider the maximum RPC data size during memory allocation for XDR strings, which allows remote attackers to cause a denial of service

**Exploitation**

*TODO: Fill out the details below. Include screenshots where possible.*

The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

* Target 1
  + flag1.txt: *TODO: Insert flag1.txt hash value*

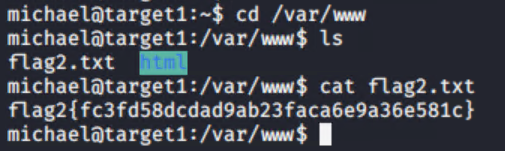
**

* + - **Exploit Used**
      * *TODO: Weak password security and open SSH port*
      * *TODO: After being able to enumerate the users through the command:*

*wpscan http://192.168.1.110/wordpress --enumerate u*

*, we established an ssh shell into Michael’s account after we guessed his password was “michael”.*

* + - * *By looking through his directories we discovered the file flag1.txt in /var/www/html directory*
  + flag2.txt: *TODO: Insert flag2.txt hash value*

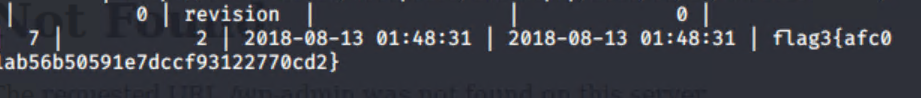
**

* + - **Exploit Used**
      * *TODO: Weak password security and open SSH port*
      * *TODO: After being able to enumerate the users through the command:*

*Wpscan http://192.168.1.110/wordpress --enumerate u*

*, we established an ssh shell into Michael’s account after we guessed his password was “michael”.*

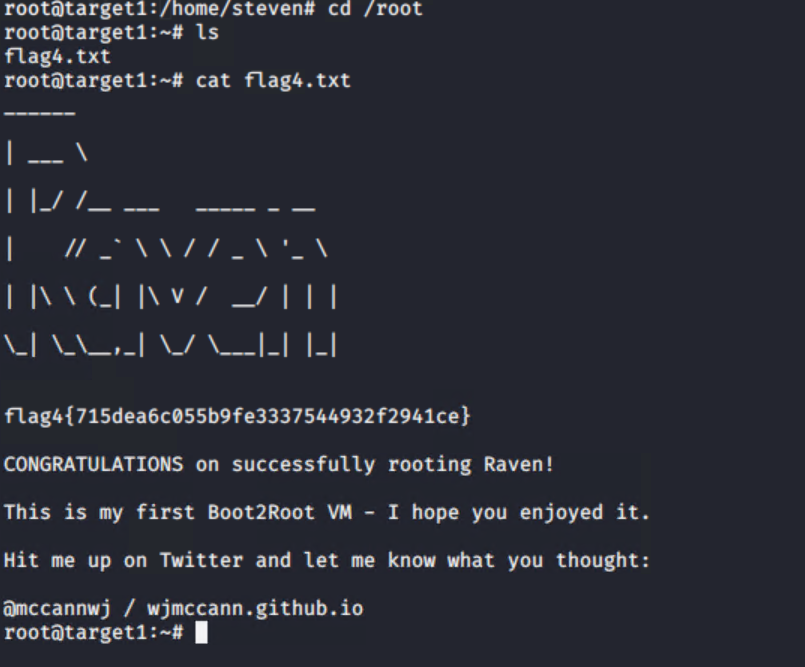
* + - * *By looking through his directories we discovered the file ‘flag2.txt’ in his /var/www directory.*
  + flag3.txt: *TODO: Insert flag3.txt hash value*



* + - **Exploit Used**
      * *TODO: Weak password security*
      * *TODO: After locating the MySQL password and username in the wp-config.php file (located in the /var/www/html folder), we gained access to the database using:*

*mysql --host=localhost --user=root --password=R@v3nSecurity.*

* + - * *Once inside the database, we were able to locate flag 3 using SELECT \* FROM wp\_posts*
  + flag4.txt: *TODO: Insert flag4.txt hash value*

**

* + - **Exploit Used**
      * *TODO: Privilege escalation*
      * *TODO: Once we cracked Steven’s password hash using John the Ripper, we established an ssh shell under his account.*
      * *Here we exploited a vulnerability and used:*

*./python -c 'import os;os.system("/bin/bash -p")'*

*to escalate to root privileges.*

* + - * *Under /root we found flag4.txt*

**Port Scanning**

* Using *nmap -sS* to scan a network and obtain ip’s of all machines on network
* Once all ip’s were obtained we used *nmap -sV* to port scan version detect

**Wordpress User Enumeration**

* Using *wpscan* we utilized it to gain username information. The username info was used by the attackers to help gain access to the web server

**Weak Passwords / Open Port 22**

* Using *nmap -sV* we scanned Target 1 and found that port 22, 80, 111, 139 and 445 which would give us access to the machine.
* With the list of users from four *wpscan* we guessed Micheal’s Password and we explored the files and found *Flags 1 & 2*.
* Alternatively you could also use *find . -iname {thisfile.txt}* to search for the flag files if they are in an area that Michael can access.
* Using *john* we also cracked stephen’s password

**MySQL Database Access**

* We were able to discover a file containing login information for the MySQL database. Able to use the login information to gain access to the MySQL database

**Misconfiguration of User Privileges/Privilege Escalation**

* We noticed that Steven had sudo privileges for python. Able to utilize Steven’s python privileges in order to escalate to root

**Apache https 2.4.10**

* Uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials

**open rpcbind port** (<https://nvd.nist.gov/vuln/detail/CVE-2017-8779#vulnCurrentDescriptionTitle> )

* rpcbind through 0.2.4, LIBTIRPC through 1.0.1 and 1.0.2-rc through 1.0.2-rc3, and NTIRPC through 1.4.3 do not consider the maximum RPC data size during memory allocation for XDR strings, which allows remote attackers to cause a denial of service